WHAT IS CLAIMED IS:

1. A method for setting passwords comprising:

(A) associating a user ID with a phone number of a personal communication device;

(B) generating a new password based at least upon a token;

(C) setting a password associated with the user ID to be the new password; and

(D) transmitting the token to the personal communication device using the phone number associated with the user ID.

2. The method of Claim 1, further comprising

(E) associating the user ID with a passcode.

3. The method of Claim 2, wherein (B) is based additionally upon the passcode.

4. The method of Claim 1, further comprising

(F) receiving a request for the user token.

5. The method of Claim 4, wherein (B), (C), and (D) are performed in response to (F).

6. The method of Claim 1, wherein the personal communication device is a mobile phone.

7. The method of Claim 1, wherein the personal communication device is a pager.

8. A password setting system comprising:

a first user database configured to associate a user ID with a phone number of a personal communication device;

a control module configured to create a password based at least upon a token, the control module further configured to cause a second user database to associate the password with the user ID; and

a communication module interface configured to cause a communication module to transmit the token to the personal communication device using the phone number associated with the user ID.

9. The password setting system of Claim 8, wherein the first user database and the second user database are the same database.

10. The password setting system of Claim 8, wherein the first user database is further configured to associate the user ID with a passcode, and wherein the control module is further configured to create the password based additionally upon the passcode.

11. A method of regulating access to a secure system, the method comprising:

(A) transmitting a user token to a personal communication device;

(B) receiving login data in response to a request for authentication information, wherein the login data is based at least upon the user token; and

(C) granting access to the secure system based upon the received login data.

12. The method of Claim 11, wherein the login data is additionally based upon a user ID.

13. The method of Claim 11, wherein the login data comprises a user ID.

14. The method of Claim 12, wherein the login data is additionally based upon a passcode.

15. The method of Claim 11, wherein the login data comprises a user ID and a password.

16. The method of Claim 15, wherein the password comprises a passcode and the token.

17. The method of Claim 16, wherein the password is a concatenation of the passcode and the token.

18. The method of Claim 16, wherein the password is a hashed concatenation of the passcode and the token.

19. The method of Claim 11, further comprising

(D) generating the user token.

20. The method of Claim 19, further comprising

(E) receiving a request for the user token.

21. The method of Claim 20, wherein (A) and (D) are performed in response to (E).

22. The method of Claim 11, wherein the personal communication device is a mobile phone.

23. The method of Claim 11, wherein the personal communication device is a pager.

24. An access control system comprising:

a user token server configured to transmit a token to a personal communication device, the user token server further configured to generate a valid password based at least upon the token; and

an authentication module configured to receive at least a submitted password in response to a request for authentication of a user, the authentication module further configured to grant access to the user if at least the submitted password is based at least upon the token and matches the valid password.

25. The access control system of Claim 24, wherein the user token server is further configured to generate the valid password based additionally upon a valid passcode that is known to the user.

26. The access control system of Claim 24, wherein the user token server is further configured to transmit the token in response to a request by the user.

27. The access control system of Claim 25, wherein the user token server is further configured to associate the valid password with a valid user ID, wherein the authentication module is further configured to receive a submitted user ID in response to the request for authentication, and wherein the authentication module is further configured to grant access to the user if, in addition, the submitted user ID matches the valid user ID.

Add B1